STEPHEN KRUEGER

Attorney at Law

P.O. Box 2060

Koror 96940

PALAU

+680 488-4887
dailidvpalau@yahoo.com.tw

February 25, 2005

Chief
Legal Division
Office of Passport Policy
Planning and Advisory Services
U.S. State Department
Washington, DC 20037
USA

Dear Sir:

I enclose my comments on the proposed regulations concerning electronic passports, RIN 1400-AB93.

Sincerely yours,

Stephen Krueger
Stephen Krueger

Certified Mail
Return Receipt Requested
No. 7004 1160 0005 0348 2559

SUBMISSION OF STEPHEN KRUEGER
CONCERNING RIN 1400-AB93
70 FED. REG. 8305 (2/18/05)

1. Proposed § 51.1(j)

a. The first sentence of the so-called definition is a description, not a definition. Substitute "'Electronic passport' means a passport with an electronic chip."

b. The second sentence is a statement of intention, not a definition. It should be stricken.

c. The Supplementary Information and the proposed regulations use certain terms without defining them: "limited passport"; "full validity passport"; "replacement passport"; "new passport"; "amended passport"; "fee passport"; "no-fee passport"; "emergency full fee passport." All key terms should be defined.

2. Proposed § 51.4(f)

a. The second sentence of the proposed regulation includes a prescription of the steps to apply for a replacement passport. That does not take into account extant prescriptions in 22 C.F.R. § 51.21 of how citizens in general apply for passports, and does not take into account extant prescriptions in 22 C.F.R. § 51.27 of how citizens who are minors under 14 apply for passports.

It is impossible to duplicate, without mistakes and unintended variances, all the details of § 51.21 and § 51.27. The prescription of the steps to apply for a replacement passport should be stricken.

b. The second sentence of the proposed regulation is unnecessary. It is obvious that a passport holder may apply again for a passport. See 22 C.F.R. § 51.21(c), § 51.21(d). The second sentence should be stricken.

3. Proposed § 51.4(h)(3)

a. The State Department wrote, "because the Department has not received the applicable fees" (emphasis added), but that is inaccurate. All applications for passports have to be accompanied by payment. See, for example, 22 C.F.R. § 51.21(c) opening paragraph, which requires submitting the "established fee" along with the passport-application paperwork.

The State Department wanted to write, but did not write, "because a negotiable instrument was tendered but payment was refused." As written, the proposal falls wide of the intended mark, so it should be stricken.

b. A regulation of this sort should be made by the Treasury Department for the government as a whole, based on expert knowledge of monetary transactions, not by an individual agency for itself, without the benefit of expert knowledge.

c. Reference was made, on Federal Register page 8307, to the possibility of a disputed credit-card charge after delivery of the passport. The State Department gets its money for the passport when it, as the merchant, gets an electronic approval for the transaction. This is done before a passport is issued. A post-transaction questioning by the citizen of the credit-card transaction causes no harm to the State Department. The proposed regulation is bottomed on the bureaucratic assumption that the State Department is always in the right, and, for that reason, no monetary dispute need be entertained by it. That is an attitude problem, and not a basis for rule-making.

d. The intended ignoring by the State Department of the possibility of an error in a credit-card transaction is contrary to 22 C.F.R. §§ 22.6, 22.7 and 23.3, which provide for refunding of fees erroneously collected by the State Department.

e. There is as well the high-handedness of the State Department to use its power to revoke passports to gain an advantage in a civil dispute.

f. The high-handedness has the additional defect of being contrary to law. There is no statutory authority for the State Department to revoke a passport in response to non-payment of a passport fee. When the Congress wanted the State Department to use passports for social-control purposes, it did so by express laws. E.g., 42 U.S.C. § 652(k) (passport revocation for non-payment of more than $5,000 in child-support obligations). The proposal has no legal grounding, so it should be stricken.

4. Proposed § 51.6

a. The proposed change would add, "or contains a damaged, defective or otherwise nonfunctioning electronic chip." This is wordy. Substitute "or contains a nonfunctioning electronic chip."

b. The State Department would add, "or has observable wear and tear that renders it unfit for further use as a travel document." The subject of the proposed rule-making is electronic passports. The proposal is outside the subject, in that wear and tear relates to the passport (e.g., a torn passport page), not to wear and tear to the chip. It was misleading for the State Department to propose a regulatory change which is outside the subject of this proposed rule-making.

Further, the State Department acted contrary to law by proposing to change this regulation absent notice (5 U.S.C. § 553(b)), the opportunity to be heard on the proposal as noticed (5 U.S.C. § 553(c)), and a statement of reasons for the proposed rule (*Schutz Comms., Inc. v. FCC*, 982 F.2d 1043, 1049 (7th Cir. 1992)). Accordingly, the proposal should be stricken.

c. The phrase, "may be invalidated" (emphasis added) gives unbridled discretion to the State Department to invalidate or not to invalidate a passport with a defective chip. A supposed regulation which does not bind an agency to do anything is no regulation at all.

d. The phrase has the additional problem of not reflecting the rule-making intention of the State Department. On Federal Register page 8306, the State Department position is that it is up to a citizen to decide whether to get a replacement passport when a chip no longer functions. Inasmuch as the proposed regulation fails to reflect the rule-making intention of the State Department, it should be stricken.

5. Proposed § 51.20

a. The proposed regulation is unnecessary, insofar as it provides "a replacement passport." In the view of the State Department, a replacement passport is issued anew, as is a first passport. Inasmuch as all passport issuances would be treated alike, there is no need, in this context, to specify "renewal passport" in addition to "a passport." Substitute "Every application for a passport . . .."

b. The proposal would drop "or for an amendment of a passport." This is inconsistent with proposed § 51.32, which would allow the State Department to consider amending a passport. If there is no regulation which permits a citizen to apply for an amendment to his passport, how does he call the attention of the State Department to his perceived need for that amendment?

c. The proposed regulation would add "extra visa pages, or other passport service." The subject of the proposed rule-making is electronic passports. The proposal is outside the subject, in that a need for extra pages is extraneous to electronic passports; and in that a need for some vague "other passport service" is extraneous to electronic passports. It was misleading for the State Department to propose a regulatory change which is outside the subject of this proposed rule-making.

Further, the State Department acted contrary to law by proposing to change this regulation absent notice (5 U.S.C. § 553(b)), the opportunity to be heard on the proposal as noticed (5 U.S.C. § 553(c)), and a statement of reasons for the proposed rule (*Schutz Comms., Inc. v. FCC*, 982 F.2d 1043, 1049 (7th Cir. 1992)). Accordingly, the proposal should be stricken.

6. Proposed § 51.32

a. This would leave it to the unbridled discretion of the State Department whether to amend a passport. A supposed regulation which does not bind an agency to do anything is no regulation at all.

b. The term "passport book" sounds odd. In any event, it is inconsistent with use of "passport" in other regulatory provisions. Further, it takes no account of the definition of "passport" in 22 C.F.R. § 51.1(e).

c. The State Department contended, on Federal Register page 8306, that neither current passports nor electronic passports should be amended or extended, to make sure that the data on the data page and the data in the chip always match. The contention overlooks the fact

that amendments and extensions are not written on data pages. They are written on the passport pages marked "Additions and Endorsements." Permitting an amendment or an extension does not interfere with the conformity of data on the chip to data on the data page, so there is no need to prohibit amendments and extensions.

7. Proposed § 51.64(b)

a. The lack of need to issue a new passport due to a change of personal data is discussed in paragraph 6(c), above. The excessive costs to citizens from the baseless proposed obligation to get a replacement passport for every intended change in a passport currently held is discussed in paragraphs 14 and 15, below.

b. The State Department proposes to rescind the present § 51.64(b), which concerns determinations of exceptional circumstances by the Secretary of State. The subject of the proposed rule-making is electronic passports. The proposal is outside the subject, in that secretarial discretion, exercised, for example, in an emergency, is unrelated to chips. It was misleading for the State Department to propose a regulatory change which is outside the subject of this proposed rule-making.

Further, the State Department acted contrary to law by proposing to change this regulation absent notice (5 U.S.C. § 553(b)), the opportunity to be heard on the proposal as noticed (5 U.S.C. § 553(c)), and a statement of reasons for the proposed rule (*Schutz Comms., Inc. v. FCC*, 982 F.2d 1043, 1049 (7th Cir. 1992)). Accordingly, the proposal should be stricken.

c. The State Department wrote, "changed his or her name or other personal identifier listed on the data page of the passport." Of the personal data listed on the data page, a citizen can change only his name. The quoted phrase should read, "changed his or her name."

8. Proposed § 51.64(c)

a. The proposal intends amelioration of the high cost of getting a replacement passports. See paragraphs 14 and 15, below. This begs the question whether the prohibition of passport amendments is necessary. See paragraph 6(c), above.

b. The one-year period is arbitrary. Why not five years? The longer the period, the lower the costs which would be imposed on citizens.

9. Proposed § 51.64(d)

The proposed change would add a new provision concerning passport issuance upon retention of a passport by law enforcement or the judiciary. The subject of the proposed rule-making is electronic passports. The proposal is outside the subject, in that criminal-case retention of a passport has nothing to do with chips. It was misleading for the State Department to propose a regulatory change which is outside the subject of this proposed rule-making.

Further, the State Department acted contrary to law by proposing to change this regulation absent notice (5 U.S.C. § 553(b)), the opportunity to be heard on the proposal as noticed (5

U.S.C. § 553(c)), and a statement of reasons for the proposed rule (*Schutz Comms., Inc. v. FCC*, 982 F.2d 1043, 1049 (7th Cir. 1992)). Accordingly, the proposal should be stricken.

10. Proposed § 51.64(e)

Suppose that a ten-year passport has a chip failure in the seventh year. A replacement passport valid for three years would be issued. That would impose on the passport holder the burden of applying again, three years later, for a ten-year passport. Done enough times by enough citizens, there is a burden as well on the State Department.

To ease the burdens, a replacement passport issued after the fifth year of validity of a ten-year passport, due to a failed chip, should be replaced with another ten-year passport. To prevent the bilking of citizens, the State Department should be required to give a credit, in an amount proportional to the remaining years of passport validity. The credit would be applicable to the passport-application fee the replacement passport.

11. Proposed § 51.66

A citizen whose passport has a failed chip, and applies for a replacement passport, would cool his heels for 4-6 weeks, the usual period for passport issuance by the State Department. To avoid this, a citizen affected by a failed chip should be entitled, without payment of the expedited-processing fee, to expedited issuance of a replacement passport.

12. Title of Subpart E

The State Department would add "or Use" to the heading of Subpart E. The subject of the proposed rule-making is electronic passports. The proposal is outside the subject, in that nothing in Subpart E relates to using electronic passports. It was misleading for the State Department to propose a regulatory change which is outside the subject of this proposed rule-making.

Further, the State Department acted contrary to law by proposing to change this regulation absent notice (5 U.S.C. § 553(b)), the opportunity to be heard on the proposal as noticed (5 U.S.C. § 553(c)), and a statement of reasons for the proposed rule (*Schutz Comms., Inc. v. FCC*, 982 F.2d 1043, 1049 (7th Cir. 1992)). Accordingly, the proposal should be stricken.

13. Proposed §§ 51.6 and 51.64(e) in relation to 22 U.S.C. § 2705

On Federal Register page 8305, the State Department wrote, "During its period of validity, a passport (when issued to a U.S. citizen for the maximum period authorized by law) is a document establishing proof of United States citizenship, pursuant to 22 U.S.C. 2705." The maximum period of validity is 10 years. 22 U.S.C. § 217a.

The quoted sentence is incorrect. Section 2705 provides that a maximum-period passport issued to a citizen is conclusive evidence of the passport holder's U.S. citizenship. The congressional directive to all U.S. government agencies, including the State Department, is to recognize the evidentiary value of a maximum-period passport for the entirety of its 10-year validity period.

Proposed § 51.6, however, would enable the State Department to unilaterally revoke a passport for an alleged failed chip. Attendant upon the unilateral revocation of a passport for that

reason would be the unilateral negation by the State Department of the § 2705 guarantee to the passport holder that his maximum-term passport has the statutory evidentiary effect. No passport means that a citizen has no ground for invoking the statutory guarantee.

Proposed § 51.64(e), which provides for issuance of a replacement passport without charge in the event of an alleged chip failure, does not remedy the negation of § 2705. The opening paragraph of proposed § 51.64 states, "A passport issuing office may issue a replacement passport . . ." (emphasis added). This is consistent with the State Department position that passport issuance is a matter of bureaucratic grace, not a matter of citizens' rights.

That being so, proposed § 51.6 purports to give to the State Department unbridled discretion to negate § 2705, and the proposed § 51.64(e) purports to give to the State Department unbridled discretion to undo its negation of § 2705. Proposed §§ 51.6 and 51.64(e) are contrary to § 2705, so they should be stricken.

14. Executive Order 12866

a. On Federal Register page 8308, the State Department projected an additional cost of $220,000 caused by implementation of electronic passports. The calculation neglected the cost of manufacturing the chip, and neglected the higher cost of producing an electronic passport as compared with the cost of producing an ordinary passport. These costs could range from $20 to $30 per passport, and the costs will be passed along by the State Department to citizens. 31 U.S.C. § 9701. About 9,000,000 passports are issued annually. 9,000,000 times $20, at the lower edge of the $20-$30 estimate, is well in excess of $100,000,000 a year.

b. The State Department estimate is that 180,000 passport applicants will have to pay the passport-related fees due to the preclusion of passport amendments. There are about 2.25 million marriages annually in the United States, and about 2.25 million divorces. The State Department estimate postulates that fewer than 10% of the more than 2 million women who are married and divorced every year change their names (i.e., assume a married name; resume a maiden name) in the process. The State Department estimate is unreasonably low, so it should not be accepted at face value.

c. The analysis of the State Department under E.O. 12866 was mistaken. The State Department may not exclude itself from E.O. 12866. The State Department should be required to apply E.O. 12866 to this proposed rule-making.

15. Small Business Regulatory Enforcement Fairness Act of 1966

a. On Federal Register page 8307, the State Department asserted that the proposed regulatory changes do not amount to a major rule; do not cause an annual economic effect of $100,000,000 or more; and do not constitute a major increase in costs or prices. As shown in paragraph 14, above, the proposed regulations would result in an annual effect on the economy in excess of $100,000,000.

b. Electronic passports would cause a major increase in the price paid by a citizen for a passport. As shown in paragraph 14, above, the cost of manufacturing the chip and the cost of producing an electronic passport would add from $20 to $30 per passport. (i) The present cost of a ten-year passport is $78 ($55 passport-application plus the $12 security charge plus $11 for photographs). Adding $20 to the $78 cost is an increase of 25%. Adding $30 to the $78 cost is an increase of 38%. (ii) The present cost of a five-year passport is $63 ($40 passport-application plus the $12 security charge plus $11 for photographs). Adding $20 to the $63 cost is an increase of 31%. Adding $30 to the $63 cost is an increase of 47%.

c. The analysis of the State Department under the Small Business Regulatory Enforcement Fairness Act was mistaken. The State Department put forward a major rule, so congressional review of the proposed rule-making is mandatory.

16. Executive Order 12988

a. The proposed regulations fail to establish clear legal standards. Shortcomings include not taking existing State Department passport regulations into account; undefined terms; inconsistency between the Supplementary Information and the intended regulations; misuse of the proposed rule-making concerning electronic passports as a vehicle for implementing unrelated regulatory changes; ignoring applicable law; and omitting passport costs pertinent to discussion of Executive Order 12866 and discussion of the Small Business Regulatory Enforcement Fairness Act of 1966.

b. The proposed regulations increase the burden on citizens by unnecessarily imposing the obligation to buy new passports to make changes in personal data, or when the State Department unilaterally directs that new passports are to be bought by citizens.

c. The analysis of the State Department under E.O. 12988 was mistaken. The State Department should apply E.O. 12988, to this proposed rule-making.

CA/PPT/PAS

2005 MAR 22 AM 10: 15

Shawn Duffy
4201 S. 31st St.
#107
Arlington, VA 22206
03/15/2005

Chief, Legal Division
Office of Passport Policy, Planning, and Advisory Services
2100 Pennsylvania Ave., NW
3rd Floor
Washington, DC 20037

Reference: RIN 1400-AB93, Comments on Electronic Passport Proposal, 22CFR51

To Whom It May Concern:

I would like to submit this letter in response to the State Department's request for comments regarding electronic passports published on 18 February 2005 in the *Federal Register*. Below, I have included all feedback regarding the proposal including requests for further information, where appropriate.

- The State Department offers three reasons for not intending to encrypt passport data. One of the reasons given ("encrypted data takes longer to read, increasing port of entry processing time") seems to warrant further explanation. The amount of data on an average passport including a small digital photo should not amount to more than 10-12 kilobytes (KB), unencrypted. When encrypted with a single 2048-bit ElGamal public encryption key, the data should still not amount to more than 15-20 KB of data (this also assumes the encrypted data would be output in ASCII format to facilitate reading by RFID readers). *Reading* encrypted data would take no longer than reading unencrypted data; 20 KB is 20 KB. It is *decrypting* the data that would require processing power and time. However, even on a moderately powerful Apple G4 PowerBook with a 1.5 GHz processor, decrypting 20 KB of ASCII-armored data encrypted with a 2048-bit ElGamal key takes less than two seconds. The time required to decrypt data that is encrypted to multiple 2048-bit or 4096-bit keys would be longer though certainly not unreasonable. If the decryption and verification process were offloaded to a moderately powerful desktop system the time would still be negligible, especially when compared with current delays at border crossings.

- The State Department also states that "encryption would require a higher level of technology and more complicated technical coordination with other nations." Can the State Department explain to what degree the above statement reflects the ITAR/EAR[1] regulations prohibiting the export of munitions including strong cryptography? If this were, in fact, a consideration, then would it not be in the best interest of the United States that other nations have access to strong cryptography in order to more fully protect legitimate passports rather than force them to use weaker technology that could potentially be forged? Further information regarding the increased level of technical complexity presented by encryption would be greatly appreciated.

- If global interoperability were a goal of the State Department's electronic passport, then it would seem to follow that non-US passports would also need to be digitally signed. If this is the case, will these passports be signed by the nation of origin? After all, how much safer are Americans if only US passports are protected against forgery? And, if other nations will be required to sign the passports of their citizens, then how does the State Department propose

[1] International Traffic in Arms Regulations/Export Administration Regulations

handling the inevitable key management problem? Any further information regarding international key management would be greatly appreciated.

- A passport is valid for ten years. When the State Department digitally signs a passport, that signature must also be valid for ten years. How does the Department intend to address the possibility of a key compromise? If a signing key were compromised, then all passports signed by that key would need to be immediately rendered invalid, whether they were legitimately signed or not. Would the State Department require all passports signed by the compromised key to be returned and re-signed? Also, in the event of a key compromise, inevitably, a certain number of US citizens will still be carrying passports with signatures from the compromised key through border checkpoints. Border agents would be able to verify the signature but they would also see that the signature is from a compromised key. If the process to re-sign passports with a valid key is not sufficiently convenient, the number of people at a given border checkpoint with invalid digital signatures is bound to increase, completely negating the added security of the signature. On the one hand, the most secure method would appear to be to keep all signing keys at a central location such as the State Department. However, this would increase the inconvenience of getting a new, valid signature, or chip, and may discourage people from doing so or, effectively preventing them from doing so in time for an international trip. On the other hand, passports could be re-signed and re-issued at border checkpoints but this would require greater dissemination of signing keys, thus increasing the likelihood of another compromise. Any further information regarding preparations for a signing key compromise would be greatly appreciated.

- In response to the issue of RFID "skimming" the proposal states "eavesdropping can only occur while the electronic chip is being read using a specially designed reader furnished with the proper public key." In terms of asymmetric cryptography, this statement would appear to be false. The "proper public key" is only needed to *verify* that data was signed by the State Department and that it has not been altered since it was signed. Without the public key, a malicious, or simply curious, person will still be able to read and/or copy the data. Any further information or clarification on this point along with more details on proposed "anti-skimming" measures would be greatly appreciated.

- The proposal states that an "electronic passport with a nonfunctioning electronic chip may continue to be used if the data page is not damaged..." While there certainly needs to be allowances for the inevitable and intermittent failures of technology, it seems that a malicious person would be able to circumvent this entire system by forging a passport and simply claiming that the chip was "damaged". The proposal states that if damage were deliberate, then the passport would be invalidated upon discovery but it is not quite clear how the State Department intends to differentiate between a deliberately damaged chip and a chip that was accidentally damaged.

Below, I have included a potential solution that would enable the State Department to encrypt the data on the electronic passport while circumventing some of the encryption problems identified in the Department's proposal.

In order to address some of major issues inherent to asymmetric cryptography, the State Department may be able to implement a *symmetric* encryption solution that would guard against RFID "skimming" and would also address key management and resource requirements (time and

processing power) inherent to asymmetric cryptography. For example, the passport number and name of the passport holder (or any standard combination of data in the passport) could be combined and then passed to a one-way hashing algorithm such as SHA-256. This process would generate a 256-bit string that could then be used to symmetrically encrypt the data on the chip by using a symmetric encryption algorithm such as Blowfish or AES-256[2]. This approach would have the following benefits:

- **Resistance to RFID skimming**: The data on the chip would be extremely resistant to RFID "skimming" and would require no further anti-skimming technology. Only those with physical access to the passport would also have access to the key. Even though the key may be vulnerable to a brute force attack since it is only a hash of potentially predictable information (name and passport number, etc), it may be easier for an attacker to physically steal the passport than it would be to break the key, especially if the attacker does not possess significant computing resources.
- **Key management is not a problem**: Data is encrypted to a single key that is known to all who have physical access to the passport. This mitigates the issue of key management. Private decryption keys are unnecessary and therefore cannot be compromised. The only key is in the passport.
- **Resource requirements (time, processing power, size) are not an issue**: Even though the resources required to decrypt a small payload encrypted with multiple public keys is negligible, the requirements in terms of computing power, time, and size of ciphertext in a symmetric encryption solution are even less demanding. Symmetric encryption with a single key is undeniably faster, requires less processing power, and limits the size of encrypted data, which is a concern on a small RFID chip.

Below is a border scenario involving symmetrically encrypted data on a RFID passport chip:

1. Janice A. American is returning from a trip abroad with her symmetrically encrypted electronic passport.
2. Simon T. Terrorist attempts to read the personal RFID information on Janice's passport by walking by her with his own RFID reader but is unable to do so because it is encrypted.
3. Janice reaches Chris Customs and hands over her passport.
4. Chris opens Janice's passport and scans the RFID chip with an RFID reader that passes the ciphertext to a desktop computer.
5. Chris reads the passport number, Janice's name, and date of birth from the passport data page.
6. Chris enters the information into the computer. This could consist of Chris manually typing in the information or scanning the information via a bar code or other non-RFID mechanism.
7. The computer takes the information, combines it and hashes it via SHA-256 or other approved one-way hashing algorithm. (This would not be necessary if the State Department included another field on the passport data page consisting of a string that meets the specification described in the footnote at the bottom of this page.)
8. The computer uses the resulting 256-bit hash to decrypt the data that has been passed to it from the RFID reader.

---

[2] For an even stronger key, the State Department could add a field to the passport data page that would contain a string of 20+ random, unique, and unpredictable alphanumeric characters. This string would then act as the symmetric encryption key and would not be vulnerable to an offline brute force attack.

9. Once the information is decrypted, the computer, armed with the State Department's public key, verifies that the data on the chip has been digitally signed by the US State Department.
10. If the signature verifies, Chris compares the information that has been decrypted and validated by his computer to the information on the passport.
11. If all information matches and both pictures appear to be Janice, Chris returns Janice's passport and allows her through.
12. Chris can be certain that Janice is who she says she is because the State Department has certified her identity with the digital signature.
13. Janice can be certain that only Chris had access to her information because any information that could be read remotely is encrypted.

National security and personal privacy are vital to American society in the 21st century and public scrutiny of government is necessary to ensure that neither is being unnecessarily sacrificed. Therefore, I would like to thank the State Department for opening this proposal to public comment, and I look forward to any future correspondence.

Sincerely,

Shawn Duffy

Email: **sduffy@codepiranha.org**
PGP Key: **getkey-sduffy@codepiranha.org**
PGP Key ID: 0x96904A68

cc: The Honorable James P. Moran, US House of Representatives
The Honorable John Warner, US Senate
The Honorable George Allen, US Senate